REMARKS

The Examiner's comments and the cited art have been noted and carefully studied. Applicants respectfully traverses the rejections and request reconsideration. For the reasons set forth below, Applicants submit the remaining claims are allowable as written.

Canceled Claims

Please cancel claims 1 and 14 without prejudice.

Amended Claims

Please amend claims 1, 3, 13 and 15 as indicated above.

Cited Reference

Yin

Yin is directed to a data security system and method. The method comprises configuring the functional elements in a hardware device to perform sequences of a data movement, bit manipulation, substitution and logical operations, which correspond to sequences in a cryptographic process, and the microprocessor for controlling the operation of a hardware device in accordance with the predetermined ordered sequence of operations in order to perform a cryptographic process on data. (col. 3, lns. 1-9). Further, Yin discloses the use of hardwired registers 70 and 72 to perform a permutation operation, (col. 6, lns. 22-42; Fig. 4), but does not disclose, teach or suggest Applicants' at least claimed subject matter that includes, inter alia, "... a register file providing operands to said arithmetic logic unit; and wherein said register file includes general purpose registers ..."

§ 102(e) Rejections

The Office Action rejected claims 1-21 under 35 U.S.C. 102(e) as being allegedly anticipated by Yin (U.S. 6,028,939).

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly, or inherently described, in a single reference. Furthermore, the identical invention must be shown in as complete detail as contained in the claim.

Applicants submit that Yin fails to disclose each and every element of Applicants' claimed subject matter and respectfully request the Examiner to withdraw the rejections. In addition, Applicants submit that Yin does not, disclose, teach or suggest, either implicitly or explicitly, Applicants' claimed subject matter.

Claim 1

Applicants submit that Yin does not disclose, teach or suggest Applicants' amended claim 1 subject matter including, inter alia,:

> "...an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations; wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and wherein said register file includes general purpose registers"

(claim 1). Applicants submit that Yin is absent any disclosure, teaching or suggestion regarding, inter alia, "...wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and wherein said register file includes general purpose registers." Applicants have reviewed the Office Action's reference to col. 7, ln. 61 – col. 8 ln. 37, which is alleged to disclose "a register file providing operands to said arithmetic logic unit," and find no disclosure to the use of a register file for any purpose including the providing of operands to an arithmetic logic unit. Further, Applicants submit that that which is disclosed col. 7, ln. 61 – col. 8 ln. 37 is limited to the structure and operation of a PHE, a hardware device, rather than a processor, i.e. a CPU, and is absent any discussion of the use of a register file or of a register file consisting of general purpose registers as claimed. In fact, the registers that are discussed in Yin, (col. 6, lns. 22-41), are hardwired registers (not general purpose registers) for performing a permutation on one of 64 stages of permutations. As such, Applicants submit that Yin's disclosed use of hardwired general purpose registers does not disclose, teach or suggest Applicants' claimed subject matter including at least either a register file or a register file containing general purpose registers.

Claim 3

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 3 subject matter including, inter alia,:

> "... said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey"

(claim 3). The Office Action makes reference to the stated language in col. 5, ln. 54 – col. 6, ln. 10 and col. 7, ln 61 – col. 8, ln 37 as disclosing Applicants' claim 3 subject matter. Applicants submit that what Yin discloses in col. 5, ln. 54 – col. 6, ln. 10 is a description of a DES operation including the dividing blocks of data into multiple parts, and the derivation of subkeys, and is otherwise absent any discussion of using a first, second and third register in the manner claimed

in Applicants' claim 3 subject matter. In addition, and as discussed above in regards to claim 2, Yin's discussion in col. 7, ln 61 – col. 8, ln 37 is directed to the operations of a PHE, and although Yin describes such PHE's as capable of being programmed to perform a number of functions and operations for data security, as well as being reconfigurable, there is no discussion therein the using a first, second and third register in the manner claimed in Applicants' claim 3 subject matter. Therefore, Applicants submit that Yin does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 3 depends from claim 1, and as a dependent claim therefrom, claim 3 is allowable for the reasons claim 1 is allowable. Applicants further submit that claim 3 is also allowable in light of the presence of novel and non-obvious elements contained in claim 3 that are not otherwise present in claim 1.

Claim 4

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 4 subject matter including, inter alia,: "... said datum is 64 bits long and said subkey is 48 bits long" (claim 4).

Applicants submit that at least because claim 4 depends from claim 3, and as a dependent claim therefrom, claim 4 is allowable for the reasons claim 3 is allowable. Applicants further submit that claim 4 is also allowable in light of the presence of novel and non-obvious elements contained in claim 4 that are not otherwise present in claim 3.

Claim 5

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 5 subject matter including, inter alia,: "... said first and second portions each contain one-half number of bits of said datum" (claim 5).

Applicants submit that at least because claim 5 depends from claim 3, and as a dependent claim therefrom, claim 5 is allowable for the reasons claim 3 is allowable. Applicants further submit that claim 5 is also allowable in light of the presence of novel and non-obvious elements contained in claim 5 that are not otherwise present in claim 3.

Claim 6

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 6 subject matter including, inter alia,: "... each of said first and second portions is 32 bits long" (claim 6).

Applicants submit that at least because claim 6 depends from claim 5, and as a dependent claim therefrom, claim 6 is allowable for the reasons claim 5 is allowable. Applicants further submit that claim 6 is also allowable in light of the presence of novel and non-obvious elements contained in claim 6 that are not otherwise present in claim 5.

Claim 7

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 7 subject matter including, inter alia,:

> "... said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent executing of said instruction."

(claim 7). Here, the Office Action makes reference to the stated language in col. 5, ln. 54 – col. 6, ln. 10 and col. 7, ln 61 – col. 8, ln 37 as disclosing Applicants' claim 7 subject matter. Applicants submit that what Yin discloses in col. 5, ln. 54 – col. 6, ln. 10 is a description of a DES operation including the dividing blocks of data into multiple parts, and the derivation of subkeys, and is otherwise absent any discussion of using a first, second and third register to "... store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent executing of said instruction." Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 7 depends from claim 3, and as a dependent claim therefrom, claim 7 is allowable for the reasons claim 3 is allowable. Applicants further submit that claim 7 is also allowable in light of the presence of novel and non-obvious elements contained in claim 7 that are not otherwise present in claim 3.

Claim 8

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 8 subject matter including, inter alia,: "... a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers" (claim 8). Here, the Office Action makes reference to the stated language in col. 5, ln. 54 – col. 6, ln. 10 and col. 7, ln 61 – col. 8, ln 37 as disclosing Applicants'

claim 8 subject matter. As discussed above, not only is such language in Yin absent from any discussion of the use of a register file generally, a register file containing general purpose registers, or first, second and third general purpose registers, Applicants further submit that Yin is also absent discussion on the use of Applicants' claimed bypass mechanism 302 – Fig. 3. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 8 depends from claim 7, and as a dependent claim therefrom, claim 8 is allowable for the reasons claim 7 is allowable. Applicants further submit that claim 8 is also allowable in light of the presence of novel and non-obvious elements contained in claim 8 that are not otherwise present in claim 7.

Claim 9

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 9 subject matter including, inter alia,: "... said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit" (claim 9). Regarding the cited to language in col. 5, ln. 54 - col. 6, ln. 10, Applicants submit that discusses a DES operation, but is otherwise absent any discussion of a "bypass mechanism," and therefore does not disclose Applicants' claimed subject matter. Similarly, Applicants submit that the cited to language in col. 7, ln. 61 to col. 8, ln. 37, describes the structure and function of a PHE, and is also absent any discussion regarding a "bypass mechanism." At least for such reasons, Applicants submit that Yin does not disclose teach or suggest Applicants' claim 9 subject matter.

Further, Applicants submit that at least because claim 9 depends from claim 8, and as a dependent claim therefrom, claim 9 is allowable for the reasons claim 8 is allowable. Applicants further submit that claim 9 is also allowable in light of the presence of novel and non-obvious elements contained in claim 9 that are not otherwise present in claim 8.

Claim 10

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 10 subject matter including, inter alia,:

> "... a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operation in parallel with said logic circuit."

(claim 10). Here, the Office Action makes reference to the stated language in col. 5, lns. 12-33 as disclosing Applicants' claim 10 subject matter. Applicants submit that what Yin discloses in col. 5, lns. 12-33 is how a DES system operates on blocks of 64 bits of data at a time in parallel

using a common algorithm and key to both encrypt and decrypt data. Applicants submit that such language in Yin, although discussing obscuring redundancies in a plaintext message in parallel, Yin does not disclose therein the performing of a key selection in parallel with a logic circuit. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 10 depends from claim 1, and as a dependent claim therefrom, claim 10 is allowable for the reasons claim 1 is allowable. Applicants further submit that claim 10 is also allowable in light of the presence of novel and non-obvious elements contained in claim 10 that are not otherwise present in claim 1.

Claim 11

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 11 subject matter including, inter alia,: "... said logic circuit further comprises a circuit for selecting a subkey from a key" (claim 11).

Applicants submit that at least because claim 11 depends from claim 1, and as a dependent claim therefrom, claim 11 is allowable for the reasons claim 1 is allowable. Applicants further submit that claim 11 is also allowable in light of the presence of novel and non-obvious elements contained in claim 11 that are not otherwise present in claim 1.

Claim 12

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 12 subject matter including, inter alia,: "... said key is 56 bits long" (claim 12).

Applicants submit that at least because claim 12 depends from claim 11, and as a dependent claim therefrom, claim 12 is allowable for the reasons claim 11 is allowable. Applicants further submit that claim 12 is also allowable in light of the presence of novel and non-obvious elements contained in claim 12 that are not otherwise present in claim 11.

Claim 13

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 13 subject matter including, inter alia,:

> "...A process for performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising: providing a logic circuit in an arithmetic logic unit; and performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit; and storing operands in a register file; and providing said operands to said logic circuit; wherein said register file includes general purpose registers."

(claim 13). Applicants submit that for the same reasons discussed above regarding the reasons why Yin does not disclose, teach or suggest Applicants' claim 1 subject matter, that Yin also does not disclose, teach or suggest Applicants' claim 13 subject matter. Namely, Applicants submit that Yin does not disclose, teach or suggest the use of "a register file providing operands to said arithmetic logic unit," and further "wherein said register file includes general purpose registers." Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Claim 15

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 15 subject matter including, inter alia,: "... storing operands in a register file; and providing said operands to said logic circuit." (claim 15).

Applicants submit that for the same or similar reasons discussed above regarding the reasons why Yin does not disclose, teach or suggest Applicants' claim 2 subject matter, that Yin also does not disclose, teach or suggest Applicants' claim 15 subject matter. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 15 depends from claim 13, and as a dependent claim therefrom, claim 15 is allowable for the reasons claim 13 is allowable. Applicants further submit that claim 15 is also allowable in light of the presence of novel and non-obvious elements contained in claim 15 that are not otherwise present in claim 13.

Claim 16

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 16 subject matter including, inter alia,:

> "... storing a first portion of a datum for said encryption or decryption in first register in said register file; storing a second portion of said datum for said encryption or decryption in second register in said register file; and storing a subkey for said encryption or decryption in third register in said register file."

(claim 16). Applicants submit that for the same or similar reasons discussed above regarding the reasons why Yin does not disclose, teach or suggest Applicants' claim 3 subject matter, that Yin also does not disclose, teach or suggest Applicants' claim 16 subject matter. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 16 depends from claim 15, and as a dependent claim therefrom, claim 16 is allowable for the reasons claim 15 is allowable. Applicants further submit that claim 16 is also allowable in light of the presence of novel and non-obvious elements contained in claim 16 that are not otherwise present in claim 15.

Claim 17

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 17 subject matter including, inter alia,:

> "... storing operands of an instruction executing on e round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction."

(claim 17). Applicants submit that for the same or similar reasons discussed above regarding the reasons why Yin does not disclose, teach or suggest Applicants' claim 7 subject matter, that Yin also does not disclose, teach or suggest Applicants' claim 17 subject matter. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 17 depends from claim 16, and as a dependent claim therefrom, claim 17 is allowable for the reasons claim 16 is allowable. Applicants further submit that claim 17 is also allowable in light of the presence of novel and non-obvious elements contained in claim 17 that are not otherwise present in claim 16.

Claim 18

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 18 subject matter including, inter alia,: "... providing said results as input to said logic circuit without first being written back to said first, second and third registers." (claim 18).

Applicants submit that for the same or similar reasons discussed above regarding the reasons why Yin does not disclose, teach or suggest Applicants' claim 8 subject matter, that Yin also does not disclose, teach or suggest Applicants' claim 18 subject matter. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 18 depends from claim 17, and as a dependent claim therefrom, claim 18 is allowable for the reasons claim 17 is allowable.

Applicants further submit that claim 18 is also allowable in light of the presence of novel and non-obvious elements contained in claim 18 that are not otherwise present in claim 17.

Claim 19

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 19 subject matter including, inter alia,: "... selecting a subkey from a key for said DES algorithm in a second logic circuit." (claim 19).

Applicants submit that at least because claim 19 depends from claim 13, and as a dependent claim therefrom, claim 19 is allowable for the reasons claim 13 is allowable. Applicants further submit that claim 19 is also allowable in light of the presence of novel and non-obvious elements contained in claim 19 that are not otherwise present in claim 13.

Claim 20

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 20 subject matter including, inter alia,: "... operating said second logic circuit in parallel with said logic circuit." (claim 20).

Applicants submit that for the same or similar reasons discussed above regarding the reasons why Yin does not disclose, teach or suggest Applicants' claim 10 subject matter, that Yin also does not disclose, teach or suggest Applicants' claim 20 subject matter. Therefore, Applicants submit that Yin cannot and does not disclose, teach or suggest Applicants' claimed subject matter.

Applicants submit that at least because claim 20 depends from claim 19, and as a dependent claim therefrom, claim 20 is allowable for the reasons claim 19 is allowable. Applicants further submit that claim 20 is also allowable in light of the presence of novel and non-obvious elements contained in claim 20 that are not otherwise present in claim 19.

Claim 21

Applicants submit that Yin does not disclose, teach or suggest Applicants' claim 21 subject matter including, inter alia,: "... selecting a subkey from a key using a key select circuit in said logic circuit." (claim 21).

Applicants submit that at least because claim 21 depends from claim 13, and as a dependent claim therefrom, claim 21 is allowable for the reasons claim 13 is allowable. Applicants further submit that claim 21 is also allowable in light of the presence of novel and non-obvious elements contained in claim 21 that are not otherwise present in claim 13.

CONCLUSION

For the foregoing reasons, withdrawal of the rejections and allowance of the remaining claims is respectfully requested. If there are any questions or comments regarding this response, the Examiner is encouraged to contact the undersigned at 312-609-7500.

Respectfully submitted,

Dated: January 28, 2004

By: _____
Brent A. Boyd
Reg. No. 51,020

Vedder, Price, Kaufman & Kammholz
222 North LaSalle Street
Chicago, Illinois 60601
Telephone: (312) 609-7500
Facsimile: (312) 609-5005